

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208986

(43)Date of publication of application : 26.07.2002

(51)Int.Cl.

H04L 29/08

H04L 12/22

H04L 29/14

(21)Application number : 2001-004772

(71)Applicant : FUJITSU LTD

(22)Date of filing : 12.01.2001

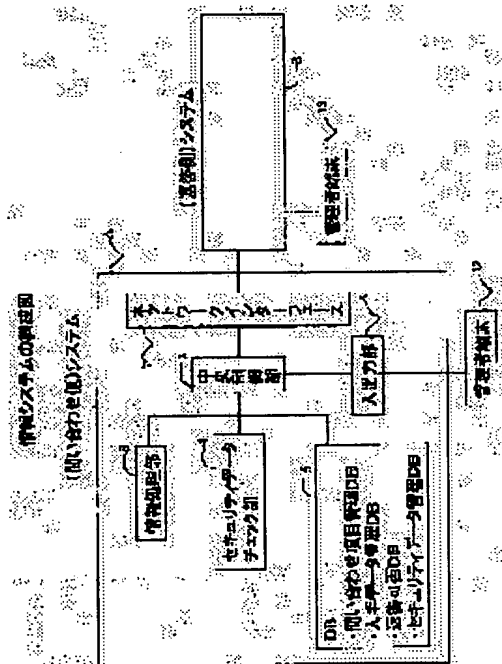
(72)Inventor : NODA TOSHITATSU
KOMURA MASAHIRO
KURODA YASUTSUGU
KOTANI MASATAKE

(54) APPARATUS AND METHOD FOR COMMUNICATING AS WELL AS MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a technique for communicating by confirming safety of a remote system of a communicating destination.

SOLUTION: An apparatus for communicating (A) electronically transmits or receives information by utilizing a network. The apparatus (A) comprises a communicating unit (7) for accessing to the network, and a controller (2) for controlling a communication. The controller (2) inquires system information of a remote apparatus (B) of the third party of transmitting and receiving the information to the remote apparatus (B), and judges whether thereafter transmission and reception is executed or not based on the system information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

【特許請求の範囲】

【請求項1】 ネットワークを利用し電子的に情報を送信または受信する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部とを備え、
前記制御部は、情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。

【請求項2】 前記システム情報には、相手装置の安全性に関連する情報が含まれており、
前記制御部は、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かを判断する請求項1記載の通信装置。

【請求項3】 前記制御部は、相手装置から入手したシステム情報に基づき相手装置を検証する請求項1記載の通信装置。

【請求項4】 前記制御部は、前記入手したシステム情報を検証するテストバケットを前記通信部から相手装置に対して送信し、そのテストバケットへのレスポンスが妥当か否かを判定することにより相手装置を検証する請求項3記載の通信装置。

【請求項5】 送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部とを備え、
前記通信部は、送信元装置からの指令を受信し、
前記制御部は、その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。

【請求項6】 ネットワークを利用し電子的に情報を送信または受信する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、
前記通信部は、送信元装置から当該通信装置に係るシステム情報の問い合わせを受信し、
前記情報管理部は、問い合わせの対象となるシステム情報を管理し、
前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記通信部から返答する通信装置。

【請求項7】 送信元装置の属性に係る情報を管理する送信元管理部をさらに備え、
前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しない請求項6記載の通信装置。

【請求項8】 送信元装置から相手装置へのシステム情

報の問い合わせに対する返答を代行する通信装置であり、

ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、

前記通信部は、送信元装置から相手装置に係るシステム情報の問い合わせを受信し、

前記情報管理部は、前記相手装置に係るシステム情報を管理し、

前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記相手装置に代わって前記通信部から返答する通信装置。

【請求項9】 ネットワークを利用し電子的に情報を送信または受信する通信方法であり、

情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、

そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有する通信方法。

【請求項10】 コンピュータに、ネットワークを利用し電子的に情報を送信または受信するさせるプログラムであり、

情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、

そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、情報通信のセキュリティに関するものである。

【0002】

【従来の技術】 従来からネットワークを利用し電子的に情報を交換する際、通信相手を確認するための認証が行われている。また、通信相手を照会し、その信頼性を確認するための与信サービス等が提供されている。また、通信経路の安全化を図るための暗号技術などが利用されている。

【0003】 さらに、システムの安全性を確認するためのチェックサービスやハッキングサービスも提供されている。これは、例えば、確認対象のシステムに対して試みにハッキングするサービスである。

【0004】 しかし、従来は、システムがその通信相手の安全性を確認する方法は提供されていなかった。このため、通信相手が認証され、あるいは通信経路の安全性が保証されても、相手相手にセキュリティホールがある場合があった。そして、その通信相手から第三者に情報が漏洩するおそれがあった。また、その通信相手を通じて第三者がなりすましをするおそれがあった。そのようなおそれのため、特定の相手システムとの情報交換が自由に行えない場合があった。

【0005】

【発明が解決しようとする課題】本発明はこのような従来の技術の問題点に鑑みてなされたものである。すなわち、本発明の課題は、通信相手の安全性を確認した上で通信する技術を提供することにある。

【0006】

【課題を解決するための手段】本発明は前記課題を解決するために、以下の手段を採用した。すなわち、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信装置（A）であり、ネットワークにアクセスする通信部（7）と、通信を制御する制御部（2）とを備え、上記制御部（2）は、情報の送受信の相手である相手装置（B）のシステム情報を当該相手装置（B）に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するものである。

【0007】好ましくは、上記システム情報には、相手装置（B）の安全性に関連する情報が含まれており、上記制御部（2）は、相手装置（B）の安全性が所定の程度に確保されているか否かを判断してもよい。

【0008】好ましくは、上記制御部（2）は、相手装置（B）の安全性が所定の程度に確保されていないと判断したときに、その事実または理由を相手装置（B）に通知してもよい。

【0009】好ましくは、この通信装置（A）は、送受信される情報の種類と問い合わせるシステム情報の項目との関係を管理する情報項目管理部（5）をさらに備え、上記制御部（2）は、送受信する情報の種類に応じて、前記情報項目管理部（5）からシステム情報の項目を選択し、相手装置（B）に問い合わせてもよい。

【0010】好ましくは、この制御部（2）は、入手済みのシステム情報を管理する入手情報管理部（5）をさらに備え、上記制御部（2）は、前記入手情報管理部（5）を参照し、その入手済みのシステム情報が相手装置（B）において更新されているか否かを問い合わせ、更新されたシステム情報と未入手のシステム情報とを入手するようにしてもよい。

【0011】好ましくは、上記入手情報管理部（5）は、システム情報の項目ごとにその情報を入手した日時を管理し、上記制御部（2）は、入手済みのシステム情報の項目にその入手日時を付加して相手装置（B）に問い合わせてもよい。

【0012】好ましくは、上記制御部（2）は、相手装置（B）から入手したシステム情報に基づき相手装置（B）を検証してもよい。

【0013】好ましくは、上記制御部（2）は、入手したシステム情報を検証するテストパケットを通信部から相手装置（B）に対して送信し、そのテストパケットへのレスポンスが妥当か否かを判定することにより相手装置（B）を検証してもよい。

【0014】また、本発明は、送信元装置（A）から相手装置（B）に電子的な情報の送信または受信を行うと

きに、送信元装置（A）の処理を代行する通信装置（22）であり、ネットワークにアクセスする通信部（7）と、通信を制御する制御部（2）とを備え、上記通信部（7）は、送信元装置（A）からの指令を受信し、制御部（2）は、その指令にしたがい、相手装置（B1、B2）に係るシステム情報を当該相手装置（B1、B2）に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するものでもよい。

【0015】好ましくは、この制御部（2）は、上記相手装置（B1、B2）に代えて、相手装置（B1、B2）の処理を代行する代理装置（24）に相手装置（B1、B2）に係るシステム情報を問い合わせるものでもよい。

【0016】また、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信装置（B）であり、ネットワークにアクセスする通信部（7）と、通信を制御する制御部（2）と、情報管理部（5）とを備え、上記通信部（7）は、相手装置（A）から当該通信装置（B）に係るシステム情報の問い合わせを受信し、情報管理部（5）は、問い合わせの対象となるシステム情報を管理し、制御部（2）は、問い合わせに応じて前記情報管理部（5）のシステム情報を検索し、通信部（7）から返答するものでもよい。

【0017】好ましくは、上記制御部（2）は、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報を返答するものでもよい。

【0018】好ましくは、上記通信装置（B）は、システム情報を更新した日時を管理する更新履歴管理部（5）をさらに備え、上記通信部（7）は、今回の問い合わせとその問い合わせに対する前回の返答日時とを受信し、上記制御部（2）は、前回の返答日時と更新した日時とを比較し、前回の返答日時以降に更新されたシステム情報を返答してもよい。

【0019】好ましくは、上記通信装置（B）は、送信元装置（A）、その送信元装置（A）が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部（5）と、システム情報を更新した日時を管理する更新履歴管理部（5）とをさらに備え、上記制御部（2）は、送信元装置（A）から問い合わせがあったときに、その問い合わせに対する返答日時とシステム情報を更新した日時と比較し、前回の返答日時の後に、更新されたシステム情報を返答してもよい。

【0020】好ましくは、上記制御部（2）は、問い合わせに対してシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しないようにしてもよい。

【0021】好ましくは、上記通信装置（B）は、システム管理者の判断を促す入出力部（6）をさらに備え、上記制御部（2）は、問い合わせに対してシステム情報

10

20

30

40

50

の返答可否を判断し、返答可否を決定できないシステム情報について、上記入出力部(6)を通じて、システム管理者に返答可否の判断を促してもよい。

【0022】好ましくは、上記通信装置(B)は、システム管理者の判断を促す入出力部(6)をさらに備え、上記制御部(2)は、問い合わせに対しシステム情報の返答可否を判断し、返答不可と判定されたシステム情報を返答をせず、返答可否を決定できないシステム情報についてシステム管理者に返答可否の判断を促してもよい。

【0023】好ましくは、上記通信装置(B)は、送信元装置(A)の属性に係る情報を管理する送信元管理部(5)をさらに備え、上記制御部(2)は、上記送信元管理部(5)を検索し、その送信元装置(A)に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しないようにしてもよい。

【0024】好ましくは、上記通信装置(B)は、システム管理者の判断を促す入出力部(6)をさらに備え、上記制御部(2)は、上記送信元管理部(5)を検索し、その送信元装置(A)に応じてシステム情報の返答可否を判断し、その送信元装置(A)に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促してもよい。

【0025】好ましくは、上記通信装置(B)は、送信元装置(A)の属性に係る情報を管理する送信元管理部(5)と、システム管理者の判断を促す入出力部(6)とをさらに備え、上記制御部(2)は、前記送信元管理部(5)を検索し、その送信元装置(A)に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報は返答をせず、返答可否を決定できないシステム情報についてはシステム管理者に返答可否の判断を促すようにしてもよい。

【0026】また、本発明は、送信元装置(A)から相手装置(B)へのシステム情報の問い合わせに対する返答を代行する通信装置(24)であり、ネットワークにアクセスする通信部(7)と、通信を制御する制御部(2)と、情報管理部(5C)とを備え、上記通信部(7)は、送信元装置(A)からの相手装置(B)に係るシステム情報の問い合わせを受信し、上記情報管理部(5C)は、相手装置(B)に係る問い合わせの対象となるシステム情報を管理し、上記制御部(2)は、問い合わせに応じて情報管理部(5C)のシステム情報を検索し、相手装置(B)に代わって通信部から返答するものでもよい。

【0027】好ましくは、上記通信部(7)は、送信元装置(A)に代えて、送信元装置(A)の処理を代行する代理装置(22)からシステム情報の問い合わせを受信し、その代理装置に返答するようにしてもよい。

【0028】また、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信方法であり、情報

の送受信の相手である相手装置(B)に係るシステム情報を当該相手装置(B)に問い合わせるステップ(S1)と、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップ(S3、S5)とを有するものでもよい。

【0029】また、本発明は、送信元装置(A)から相手装置(B1、B2)に電子的な情報の送信または受信を行うときに、送信元装置(A)の処理を代行する通信方法であり、送信元装置(A)からの指令を受信するステップ(S100)と、その指令にしたがい、相手装置(B1、B2)に係るシステム情報を当該相手装置(B1、B2)に問い合わせる問い合わせステップ(S101)と、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップ(S103、S105)とを有するものでもよい。

【0030】また、本発明は、ネットワークを利用し電子的に情報を送信または受信させる通信方法であり、送信元装置(A)からシステム情報の問い合わせを受信する受信ステップ(S1)と、問い合わせに対するシステム情報を検索するステップ(S22、S23)と、そのシステム情報を返答する返答ステップ(S28)とを有するものでもよい。

【0031】また、本発明は、送信元装置(A)から相手装置(B1、B2)へのシステム情報の問い合わせに対する返答を代行する通信方法であり、送信元装置(A)からの相手装置(B1、B2)に係るシステム情報の問い合わせを受信する受信ステップ(S101)と、問い合わせに応じて、相手装置(B1、B2)に係るシステム情報を検索するステップ(S102)と、相手装置(B1、B2)に代わって通信部から返答するステップ(S102)とを有するものでもよい。

【0032】また、本発明は、コンピュータに以上の機能を実現させるプログラムをコンピュータ読み取り可能な記録媒体に記録したものでもよい。

【0033】以上述べたように、本発明によれば、通信相手のセキュリティレベルをチェックできるようになり、情報交換をする際の、通信相手を通じた情報の漏洩やなりすましによる不正アクセスの危険が軽減される。さらにこのようなシステム情報の管理をデータベースを利用して自動化することにより、管理者の負担が軽減される。

【0034】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

【0035】《第1実施形態》本発明の第1実施形態を図1から図11の図面に基いて説明する。

【0036】図1は、セキュリティレベルの確認を行う情報システムの構成図であり、図2は、図1に示した問い合わせ項目管理データベースのデータ構造を示す図であり、図3は、問い合わせ側のシステムが一度入手した

10

20

30

40

50

データを管理する入手データ管理データベースのデータ構造を示す図であり、図4は、図1に示した返答側のシステムが問い合わせに対する返答の可否を判断するための返答可否データベースのデータ構造を示す図であり、図5は、返答側のシステムが返答するセキュリティデータを管理するセキュリティデータ管理データベースのデータ構造を示す図であり、図6は問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートであり、図7は、図6に示したセキュリティデータの問い合わせ処理の詳細を示すフローチャートであり、図8は、図6に示したセキュリティデータの返答処理の詳細を示すフローチャートであり、図9は、図6に示したセキュリティ判定処理の詳細を示すフローチャートであり、図10は、第1実施形態の変形例における返答履歴管理データベースのデータ構造を示す図であり、図11は、第1実施形態の変形例における情報を過去に提供した日時と変更した日時を確認する処理を示す図である。

【0037】<システム構成>図1は、システム間の情報授受に際して、セキュリティレベルの確認を行う情報システムの構成図である。この情報システムは、情報を提供するシステムAと、情報の提供を受けるシステムBと、管理者端末12および13とから構成される。

【0038】システムAは、例えば、パーソナルコンピュータにより構成される。システムAは、情報提供に際して、提供先のセキュリティレベルを判定するため、予め情報提供先（これを情報入手側ともいう）にセキュリティデータを問い合わせる。このような問い合わせを行うシステムを問い合わせ側システムと呼ぶ。

【0039】一方、情報の提供を受けるシステムBは、この問い合わせに返答する。本実施形態では、このようなシステムを返答側システムと呼ぶ。このシステムBも、例えば、パーソナルコンピュータにより構成される。

【0040】また、システムBは、情報受信後に、受信した情報が信用できるか否かを判断するため、システムAにセキュリティデータを問い合わせる。したがって、システムBは問い合わせ側システムとしても機能する。

【0041】また、このとき、システムAは、その問い合わせに返答する。したがって、システムAは、返答側システムとしても機能する。

【0042】システムAおよびシステムBは、各々管理者端末12および13に接続されている。そして、システムAにおいて判断できない問題は、管理者端末12に転送される。また、システムBにおいて判断できない問題は、管理者端末13に転送される。このような問題は、各管理者の判断に委ねられる。

【0043】図1のように、システムAは、システムAの各構成要素を制御する中央制御部2と、情報処理のためのアプリケーションプログラムから構成され情報処理を実行する情報処理部3と、情報入手側のセキュリティ

レベルを判定するセキュリティデータチェック部4と、各種の情報を提供するデータベース5と、管理者端末12との通信を行う入出力部6と、ネットワークにアクセスし、情報提供先のシステムB等と通信するネットワークインターフェース7とを有している。

【0044】中央制御部2は、いわゆるCPUであり、各種のプログラムを実行し、システムAの機能を提供する。

【0045】情報処理部3は、不図示のメモリ上にロードされ、中央制御部2で実行される各種のアプリケーションプログラムである。これらのアプリケーションプログラムには、例えば、システムBとの通信を実行するプログラム等が含まれる。

【0046】セキュリティデータチェック部4は、情報処理部3から情報を提供される提供先、例えば、システムBにセキュリティデータを問い合わせ、そのセキュリティレベルを判定する。

【0047】データベース5は、問い合わせ項目管理データベースおよび入手データ管理データベースを含んでいる。これらのデータベースは、システムAが問い合わせ側システムとして機能するときに使用される。

【0048】問い合わせ項目管理データベースは、セキュリティデータチェック部4が返答側システムに問い合わせるセキュリティデータの項目を管理する。また、入手データ管理データベースは、過去に返答側システムから返答されたセキュリティデータを管理する。

【0049】さらに、データベース5は、返答可否データベースおよびセキュリティデータ管理データベースを含んでいる。これらのデータベースは、システムAが返答側システムとして機能するときに参照される。

【0050】返答可否データベースは、問い合わせ側システムから問い合わせのあったセキュリティデータ等を問い合わせ側システムに返答することの可否を判定するために使用される。

【0051】また、セキュリティデータ管理データベースは、システムA自身のセキュリティデータを管理する。このデータベースでは、問い合わせへの返答対象となる情報が管理される。

【0052】入出力部6は、中央制御部2からの指令により管理者端末12との通信を実行する。ネットワークインターフェース7は、中央制御部2からの指令によりシステムB等と通信する。

【0053】システムBの構成は、システムAの構成と同様である。そこで、システムBの構成については、説明を省略する。

【0054】<データ構造>図2に問い合わせ項目管理データベースのデータ構造を示す。システム間の情報授受において、情報提供元のシステム（問い合わせ側システムに該当）は、情報を提供する前に、このデータベースを参照し、その情報入手側のシステム（返答側システ

10

20

30

40

50

ムに相当)に問い合わせる項目を決定する。

【0055】また、情報の提供を受けたシステム(問い合わせ側システムに該当)は、情報を入手後、その情報が信用できるか否かを判定するために、このデータベースを参照し、情報提供側のシステム(返答側システムに相当)に問い合わせる項目を決定する。

【0056】問い合わせ項目管理データベースは、テーブル形式で構成される。このテーブルの各行は、授受される情報の種類と必要なセキュリティデータ項目のフィールドを有している。

【0057】授受される情報の種類には、例えば、“1000万円未満の取引”、“1000万円以上の取引”、“関係者外秘情報”、“情報A”等のように、授受される情報の区分が記述される。

【0058】一方、必要なセキュリティデータ項目には、例えば、“OS”、“パスワード暗号化”、“ログ監査”、“項目A”、“開いているポート”、“ウィルス対策”等が列記される。

【0059】ここで、“OS”とは、OSの種類を問い合わせることの指定である。また、“パスワード暗号化”とは、パスワード暗号化機能の有無を問い合わせることの指定である。

【0060】“ログ監査”とは、蓄積された通信ログを監査する監査機能の有無や監査の頻度を問い合わせることの指定である。“開いているポート”とは、受信したデータを処理するアプリケーション層プロトコルが設定されているポート番号を問い合わせることの指定である。

【0061】図2では、“1000万円未満の取引”の行には、“OS”および“パスワード暗号化”が必要なセキュリティデータの項目として指定されている。この場合、問い合わせ側システムは、1000万円未満の取引に関する情報を提供する場合、その情報提供先にOSの種類、およびパスワード暗号化機能の有無を問い合わせる。

【0062】図3に入手データ管理データベースのデータ構造を示す。このテーブルは、問い合わせ側システムが返答側システムから入手したセキュリティデータを管理するために使用される。

【0063】この入手データ管理データベースは、テーブル形式で構成される。このテーブルの各行は、返答側システム、項目、入手日時、入手セキュリティデータの各フィールドを有している。

【0064】返答側システムは、入手データを返答したシステムを一意に特定する情報である。これは、例えば、ネットワーク上のホスト名である。ホスト名の代わりに、IP(Internet Protocol)アドレスやMAC(Media Access Control)アドレスを用いてシステムを記述してもよい。

【0065】項目は、入手したセキュリティデータの種

類である。これは、例えば、“OS”、“開いているポート”、“ログ監査頻度”、“項目A”、“パスワード暗号化”等である。

【0066】入手日時は、その情報を入手した年月日と時刻である。入手セキュリティデータには、入手されたデータを記述する。例えば、項目“OS”に対して、Windows NT SP5(Windows NTは、米国マイクロソフト社の商標である)が記録される。また、項目“開いているポート”に対して7、23、80等が記録される。また、項目“ログ監査頻度”に対して、1回/1日が指定される。

【0067】図4に、返答可否データベースのデータ構造を示す。このデータベースは、返答側システムにおいて、問い合わせに対する返答の可否を判断するために使用される。この返答可否データベースは、テーブル形式で構成される。

【0068】このテーブルの各行は、問い合わせ側システム、項目、および判断の各フィールドを有している。

【0069】問い合わせ側システムは、問い合わせ側のシステムを一意に特定する情報である。また、項目は、問い合わせの対象であるセキュリティデータの種類である。判断には、返答の可否が記述される。

【0070】図4では、例えば、システムAからの項目“OS”に対する問い合わせに対して、×、すなわち、返答不可であることが指定されている。また、システムAからの項目“開いているポート”に対する問い合わせに対して○、すなわち、返答可が指定されている。

【0071】また、システムCからの項目“OS”に対する問い合わせに対して、△、すなわち、判断不可が指定されている。この場合、返答側システム、例えばシステムBは、管理者端末13に返答可否の判断を問い合わせ、管理者の指示を受けることになる。

【0072】図5にセキュリティデータ管理データベースのデータ構造を示す。このデータベースは、返答側システムが、セキュリティデータを管理するために使用される。返答側システムは、問い合わせ側システムからの問い合わせに対して、このデータベースを参照して返答する。

【0073】セキュリティデータ管理データベースは、テーブル形式で構成される。このテーブルの各行は、項目、セキュリティデータおよび更新日時の各フィールドを有している。

【0074】これらのうち、項目およびセキュリティデータは、図3に示した入手データ管理データベースの項目および入手セキュリティデータと同様であるので、その説明を省略する。

【0075】また、更新日時は、各セキュリティデータの更新日時である。図5では、例えば、この返答側システムのOSが2000年1月13日11時0分に更新され、Windows NT SP5になったことが分かる。また、“開

10

20

30

40

50

いているポート”が2000年3月31日12時24分に7、23、80に設定されたことが分かる。

【0076】<作用と効果>図6に、情報提供側であるシステムAと情報入手側であるシステムBとの通信手順を示す。図6では、システムAがシステムBに情報を提供する前に、システムBのセキュリティを検証する。そのセキュリティが充分であると確認された場合、システムAがシステムBに情報を提供する。

【0077】一方、システムBは、逆にシステムAのセキュリティを検証することで、入手した情報が信用できるか否かを確認する。

【0078】図6では、まず、システムAがシステムBにセキュリティデータを問い合わせる(S1)。すると、システムBが対応するセキュリティデータを返答する(S2)。

【0079】次に、システムAは、セキュリティ判定処理を実行する(S3)。すなわち、システムAは、返答されたセキュリティデータを基に、システムBのセキュリティが充分か否かを判定する。システムBのセキュリティが充分でない場合(S3でNGの場合)、システムAは、処理を終了する。

【0080】一方、セキュリティが充分である場合(S3でOKの場合)、システムAは、入手したセキュリティデータを検証するためのテストパケットを送信する(S4)。そして、テストパケットに対するレスポンスにより、セキュリティデータが正しいか否かを判断する(S5)。

【0081】これは、例えば、入手したセキュリティデータの項目が”開いているポート”であり、入手したデータが7、23、80の場合、そのポート番号のパケットを送信し、応答が返るか確認する処理である。また、そのポート番号以外のパケットに対して応答がないことを確認してもよい。

【0082】また、相手システムのOSの種類の入手するアプリケーションとして、例えば、nmapが知られている。nmapは、インターネット上のホームページ、<http://www.insecure.org/nmap/index.html>で解説されている。nmapは、例えば、相手システムに対して、telnetやftpのようなアプリケーション層に接続されるポートにパケットを送信し、そのシステムにログインする前に返送されるバナーを収集する。そのような手順により、nmapは、相手システムのOSの種類を入手する。そのようなバナーには、OSの種類やバージョンが含まれるからである。

【0083】また、パスワードの暗号化の有無、ログ監査の頻度等に関しては、システムの監査を行う第三者機関に問い合わせる。情報の提供側システムと提供先システムは、自身の監査を行う第三者機関を互いに相手に通知しておけばよい。

【0084】以上のようなテストパケット確認の結果、

セキュリティデータが正しくなかった場合、システムAは、処理を終了する。一方、セキュリティデータが正しいことが確認された場合、システムAは、情報提供を行う(S6)。これは、例えば、取引情報の送信、関係者外秘情報の送信、特定の情報の送信等である。

【0085】その結果、システムBは、その情報を入手する(S7)。次に、システムBは、システムAにセキュリティデータを問い合わせる(S8)。入手した情報が信用できるか否かを確認するためである。

【0086】これに対して、システムAは、セキュリティデータを返答する(S9)。すると、システムBは、入手したセキュリティデータによりシステムAのセキュリティを確認するため、セキュリティ判定処理を実行する(SA)。

【0087】その結果、システムAのセキュリティが不十分な場合(SAの処理結果がNGの場合)、システムBは処理を終了する。一方、システムAのセキュリティが十分な場合(SAの処理結果がOKの場合)、セキュリティデータを検証するためのテストパケットをシステムAに送信する(SB)。そして、システムBは、セキュリティデータが正しいか否かを確認する(SC)。SBおよびSCの処理は、システムAにおけるS4-S5の処理と同様である。

【0088】SCの判定における確認の結果、システムAのセキュリティデータが正しくなかった場合、システムBは、処理を終了する。一方、システムAのセキュリティデータが正しいことを確認できた場合、システムBは提供されたセキュリティデータを信用し、利用する。

【0089】図7に、セキュリティデータの問い合わせ処理(図6のS1またはS8)の詳細を示す。いま、図7では、システムAからシステムBに問い合わせる場合(図6のS1の処理)を仮定する。

【0090】まず、問い合わせ側のシステムAは、問い合わせ項目管理データベースを参照し、送受信する情報内容に応じて問い合わせるセキュリティデータの項目を決定する(S11)。

【0091】次に、システムAは、問い合わせるセキュリティデータの項目が入手データ管理データベースに登録されているか否かを判定する(S12)。入手データ管理データベースには、過去に問い合わせられたセキュリティデータの項目がそのセキュリティデータの入手日時とともに記録されている。

【0092】そして、システムAは、入手データ管理データベースに登録されている項目については、その項目に対応するデータが変更されているか否かをシステムBに問い合わせる(S13)。この問い合わせは、その問い合わせ項目に前回データを入手した日時(時間データ)を付して行う。

【0093】一方、入手データ管理データベースに登録されていない項目については、システムAは、そのまま

システムBに問い合わせる(S14)。以上は、システムAからシステムBに問い合わせる場合(図6のS1の処理)を仮定して説明したが、システムBからシステムAに問い合わせる場合(図6のS8の処理)も同様である。

【0094】図8に、セキュリティデータ返答処理(図6のS2またはS9の処理)の詳細を示す。図8では、システムBからシステムAにセキュリティデータを返答する場合(図6のS2の処理)を仮定して説明する。

【0095】まず、システムBは、問い合わせ元のシステムをチェックし、問い合わせ元がシステムAであることを認識する(S21)。次に、システムBは、問い合わせ項目をチェックする(S22)。

【0096】次に、システムBは、返答可否データベースを参照し(S23)、問い合わせ元と問い合わせ項目との組み合わせが返答可能なものか否かを判定する(S24)。そして、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて”返答してよい”と規定されている場合、システムBは、セキュリティデータ管理データベースを参照し、問い合わせの対象となっている項目のセキュリティデータを参照する(S26)。

【0097】次に、過去においてセキュリティデータが提供された日時がその問い合わせに付加されている場合、システムBは、過去に提供された日時とそのセキュリティデータがシステムBで変更された日時とを確認する(S27)。

【0098】そして、そのセキュリティデータが過去に提供されていないか(初めて提供されるデータか)、または、過去に提供されたデータでその後変更されたものである場合、システムBはそのセキュリティデータを返答する(S28)。

【0099】一方、そのセキュリティデータが過去にシステムAに提供された後、変更されていない場合、システムBはシステムAに変更なしという返答を行う(S29)。

【0100】また、S24の判定で、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて”返答してはいけない”と規定されている場合、システムBは、問い合わせ対象のセキュリティデータを返答できないとシステムAに返答する(S2A)。

【0101】また、S24の判定で、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて返答の”可否を判断できない”と規定されている場合、システムBは、管理者端末13に返答可否を問い合わせるメッセージを送信し、管理者の指令を求める(S25)。

【0102】管理者からの指令が”返答してよい”というものである場合、システムBは、S26以下の処理により、システムAに返答する。一方、管理者からの指令

が”返答してはいけない”というものである場合、システムBは、システムAに返答できないと返答する(S2A)。

【0103】図9に、セキュリティ判定処理(図6のS4の処理)の詳細を示す。図9では、システムAから入手した情報をシステムBが判定する場合について説明する。

【0104】まず、システムBは、システムAからのセキュリティデータの項目に関する返答内容をチェックする(SA1)。次に、システムBは、入手データ管理データベースに返答内容と入手日時を登録する(SA2)。

【0105】次に、システムBは、返答内容に問題がないか否かを判定する(SA3)。これは、返答内容からシステムAのセキュリティレベルを判定する処理である。返答内容に問題がない場合(SA3の処理結果が”問題ない”の場合)、システムBは、システムAのセキュリティレベルが充分である(OK)と判定する(SA5)。

【0106】また、返答内容に問題がある場合(SA3の処理結果が”問題あり”の場合)、システムBは、セキュリティレベルが不充分である事実および理由を相手(システムA)に通知する(SA6)。これにより、システムBは、本処理結果をNGと判定する。

【0107】また、返答内容に問題があるか否かが分からない場合(SA3の処理結果が”分からない”の場合)、システムBは、管理者端末13にシステムAのセキュリティレベルの判断を求めるメッセージを送信し、管理者の判断を求める(SA4)。

【0108】管理者の判断が”問題ない”の場合、システムBは、システムAのセキュリティレベルが充分である(OK)と判定する(SA5)。一方、管理者の判断が”問題あり”の場合、システムBは、セキュリティレベルが不充分である事実および理由を相手(システムA)に通知する(SA6)。これにより、システムBは、本処理結果をNGと判定する。

【0109】以上述べたように、本実施形態の情報システムによれば、情報の送受信の相手である相手システムのセキュリティデータを当該相手システムに問い合わせる。そして、各システムは、そのセキュリティデータに基づいて、それ以降の送受信を行うか否かを判断する。その結果、相手システムのセキュリティレベルが不充分な状態での通信の継続を回避できる。

【0110】また、本情報システムによれば、返答側のシステムのセキュリティレベルが不充分であると判断された場合、問い合わせ側のシステムは、その事実および理由を返答側のシステムに通知する。これにより、返答側システムは、自身のセキュリティ上の欠陥を認識できる。

【0111】また、本情報システムによれば、授受され

る情報に応じて必要なセキュリティ項目が問い合わせ項目管理データベースに定義される。これにより、各システムは、授受される情報に応じて適切な問い合わせ項目を決定できる。

【0112】また、本情報システムによれば、上記回答側システムは、問い合わせ側システムからの問い合わせに対して返答するセキュリティデータを管理するセキュリティデータ管理データベースを有している。これにより、回答側システムは、返答すべきセキュリティデータを一元的に管理できる。

【0113】また、本情報システムによれば、回答側システムは、問い合わせに対する返答の可否を判断する返答可否データベースを有している。これにより、回答側のシステムは、問い合わせに返答すべきか否か、またはその判断できないかを、問い合わせ側システムと問い合わせ内容の関係から導くことができる。

【0114】また、本実施形態では、問い合わせ側システムは、回答側システムから入手したセキュリティデータを管理する入手データ管理データベースを有している。これにより、問い合わせ側システムは、過去に問い合わせたセキュリティデータについては、入手日時を付加して回答側システムに問い合わせることができる。

【0115】また、回答側サブシステムは、上記セキュリティデータ管理データベースに各セキュリティデータの更新日時を有している。その結果、回答側システムは、問い合わせのあったセキュリティデータうち、更新があったセキュリティデータ、また、初めて問い合わせのあったセキュリティデータに限定して返答することができる。

【0116】また、本情報システムによれば、回答側システム、例えばシステムBは、管理者端末13に接続され、問い合わせに対する返答の可否を判断できない場合、返答可否の判断を求めるメッセージを管理者端末13に送信することができる。したがって、返答可否の判断が困難な問題については、その判断を管理者に委ねることができる。判断の難易に応じて柔軟な対応ができる。

【0117】また、本実施形態では、セキュリティデータを問い合わせたシステム、例えばシステムBは、そのセキュリティデータから相手システムのセキュリティが充分か否かを判断できない場合、その判断を求めるメッセージを管理者端末13に送信することができる。したがって、セキュリティレベルの良否の判断が困難な場合においては、その判断を管理者に委ねることができ、判断の難易に応じて柔軟な対応ができる。

【0118】また、返答可否の判断が困難な問題以外については、上記データベースの検索結果に基づいてシステムが処理する。このため、管理者の負担を軽減することができる。

【0119】＜変形例＞上記実施形態では、問い合わせ側システム、例えば、システムAがセキュリティデータ

を問い合わせる際、入手データ管理データベースを参照し、過去に問い合わせた日時をその問い合わせに付加した。

【0120】しかし、本発明の実施は、このような構成や作用に限定されない。例えば、回答側システム、例えば、システムBにおいて過去に返答した内容を記録する返答履歴管理データベースを有し、セキュリティデータ管理データベースの変更履歴と比較して、変更のあったセキュリティデータを返答するようにしてもよい。

【0121】図10に返答履歴管理データベースのデータ構造を示す。このデータベースの構造は、図3に示した入手データ管理データベースと同様である。この返答履歴管理データベースは、テーブル形式で構成される。このテーブルの各行は、問い合わせ側システム、項目、返答日時、返答セキュリティデータの各フィールドを有している。

【0122】問い合わせ側システムは、セキュリティデータを問い合わせたシステムを一意に特定する情報である。項目は、返答されたセキュリティデータの種類である。返答日時は、その情報を返答した年月日と時刻である。返答セキュリティデータには、返答されたデータを記述する。

【0123】図11に、この返答履歴管理データベースを用いて、過去に返答をした日時（過去に提供した日時）と変更した日時を確認する処理（図8のS27に代わる処理）を示す。

【0124】問い合わせを受信した回答側システム、例えばシステムBは、返答履歴管理データベースを参照し（S271）、その問い合わせにすでに返答済みであるか否かを判定する（S272）。その問い合わせに対してセキュリティデータが、その問い合わせ側システムに返答済みでない場合、システムBは、S28の処理（図8）に制御を進める。これにより、問い合わせのあったセキュリティデータが返答される。

【0125】一方、その問い合わせ側システムに対してセキュリティデータが返答済みである場合、システムBは、セキュリティデータ管理データベース（図5）の更新日時を参照する（S273）。そして、その更新日時を返答履歴データベースの返答日時と比較する（S274）。

【0126】更新日時が返答日時より後である場合、システムBは、S28の処理（図8）に制御を進める。これにより、問い合わせのあったセキュリティデータが返答される。

【0127】また、更新日時が返答日時より後でない場合、システムBは、S29の処理（図8）に制御を進める。これにより、変更なしという返答が問い合わせ側システムに送信される。

【0128】《第2実施形態》図12から図17を参照して本発明の第2実施形態を説明する。図12は、第2

実施形態に係る情報システムのシステム構成図であり、図13は、図12に示した返答側代理指定データベース23のデータ構成を示す図であり、図14および図15は、第2実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートであり、図16および図17は、第2実施形態の変形例に係る情報システムのシステム構成図である。

【0129】上記第1実施形態では、情報提供に際して、提供先のシステムBのセキュリティレベルを判定し、セキュリティに問題がないシステムBに対して情報を提供するシステムAについて説明した。

【0130】また、その場合に情報の提供を受けたシステムBがその情報が信用できるか否かをシステムAのセキュリティレベルを判定することによって確認する処理についても説明した。

【0131】上記のような相手システムのセキュリティを判定するため、システムAは、システムBに対して必要なセキュリティデータを問い合わせた。また、システムBも、入手した情報が信用できるか否かを確認するために、システムAのセキュリティデータを問い合わせた。

【0132】本実施形態では、このようなセキュリティデータの問い合わせまたは返答を代理システムを通じて授受する例について説明する。他の構成および作用は第1実施形態と同様である。そこで、同一の構成については、同一の符号を付してその説明を省略する。また、必要に応じて図1から図11の図面を参照する。

【0133】＜システム構成＞図12に本実施形態における情報システムのシステム構成図を示す。この情報システムは、問い合わせ側のシステムAと、問い合わせ側代理システム22と、返答側代理システム24と、返答側のシステムB1、B2等から構成される。

【0134】システムAは、システムB1、B2等に情報を提供する場合、提供する情報の種類を問い合わせ側代理システム22に通知する。ここで、システムAを代理する問い合わせ側代理システム22は、問い合わせ側代理指定ファイル21に定義されている。

【0135】すると、問い合わせ側代理システム22は、問い合わせ項目管理データベース5Aを参照し、第1実施形態の場合におけるシステムAと同様、情報提供先のシステム（システムB1、B2等）に問い合わせるセキュリティデータの項目を決定する。

【0136】次に、問い合わせ側代理システム22は、問い合わせるセキュリティデータの項目が入手データ管理データベース5Bに格納されているか否かを検索する。そのセキュリティデータの項目が入手データ管理データベース5Bに格納されている場合、そのセキュリティデータの入手日時を検索する。そして、問い合わせ側代理システム22は、その日時を付して問い合わせを行う。

【0137】また、このとき、問い合わせ側代理システム22は、直接システムB1、B2等に問い合わせることをせず、返答側代理システム24に問い合わせる。B1、B2等の返答側代理システム24は、返答側代理指定データベース23に定義されている。

【0138】すると、返答側代理システム24は、問い合わせの対象であるシステムB1、B2等に代わって、そのセキュリティデータを問い合わせ側代理システム22に返答する。このとき、返答側代理システム24の処理は、第1実施形態におけるシステムBと同様である。

【0139】すなわち、返答側代理システム24は、問い合わせ対象のシステムごとに構成されたセキュリティデータ管理データベース5Cおよび問い合わせ可否データベース5Dを参照し、問い合わせ側のシステムAに対して返答可とされているセキュリティデータを返答する。

【0140】返答されたセキュリティデータを受信した問い合わせ側代理システム22は、返答されてセキュリティデータを入手データ管理データベース5Bに格納する。さらに、問い合わせ側代理システム22は、そのセキュリティが充分か否かを判定し、システムAに返答する。

【0141】＜データ構成＞図13に返答側代理指定データベース23の構成を示す。このデータベースは、テーブル形式で構成される。この表の各行は、返答側システムおよび返答側代理システムの各フィールドを有している。

【0142】この返答側システムのフィールドには、返答側システムをユニークに識別する情報が指定される。また、返答側代理システムのフィールドには、返答側代理システムをユニークに識別する情報が指定される。

【0143】図13では、例えば、返答側システムB1、およびB2の返答側代理システムとして、各々D1が指定されている。また、返答側システムB3の返答側代理システムとして、各々D2が指定されている。このように、返答側代理システムは、複数の返答側システムの代理となつてよい。

【0144】そのため、図12に示した、セキュリティデータ管理データベース5Cおよび応答可否データベース5Dは、代理される返答側のシステムB1、B2ごとにデータを保持する。

【0145】図12に示した問い合わせ側代理指定ファイル21には、自身（例えば、システムAの）問い合わせ側代理システムを識別する情報が少なくとも1つ定義される。これは、例えば、問い合わせ側代理システム22のホスト名、IPアドレス、MACアドレス等である。

【0146】＜作用と効果＞図14および図15に、本実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートを示す。な

お、図14および図15において、問い合わせ側代理システムV、Xとは、図12における問い合わせ側代理システム22と同様の機能を提供するシステムである。また、図14および図15において、返答側代理システムW、Yとは、図12における返答側代理システム24と同様の作用をするシステムである。

【0147】図14のフローチャートは、情報を提供するシステムAが問い合わせ側代理システムVおよび返答側代理システムWにより、情報の提供先であるシステムBに関するセキュリティレベルを判定する処理を示している。

【0148】この処理では、システムAは、情報提供先のシステムBと提供する情報の種類とを添付し、問い合わせ側代理システムVにセキュリティデータの問い合わせを依頼する(S100)。

【0149】すると、問い合わせ側代理システムVは、セキュリティデータの問い合わせ処理を実行する(S101)。この処理は、第1実施形態に示したS1の処理とほぼ同様である。ただし、問い合わせ側代理システムVは、応答側代理指定データベース23に定義された返答側代理システムWに問い合わせを発信する。

【0150】すると、返答側代理システムWは、問い合わせの対象であるシステムBにおけるセキュリティデータを返答する(S102)。この処理は、図6に示したS2の処理と同様である。

【0151】すると、問い合わせ側代理システムVは、セキュリティ判定処理(S103)およびセキュリティデータを検証するためのテストパケットの送信を実行する(S104)。

【0152】次に、問い合わせ側代理システムVは、テストパケットに対する応答からセキュリティデータが正しいか否かを判定する(S105)。セキュリティデータが正しい場合、問い合わせ側代理システムVは、その旨をシステムAに回答する。その結果、システムAは、システムBに情報提供をする(S106)。

【0153】図15は、入手した情報が信用できるか否かを、問い合わせ側代理システムXおよび返答側代理システムYによってシステムBが判定する処理を示すフローチャートである。

【0154】システムBは、入手した情報の種類と入手先を添付してセキュリティデータの問い合わせを問い合わせ側代理システムXに依頼する(S10E)。すると、問い合わせ側代理システムXは、セキュリティデータの問い合わせ処理を実行する(S108)。すると、返答側代理システムYは、問い合わせ対象のセキュリティデータを返答する(S109)。

【0155】これに対して、問い合わせ側代理システムXは、セキュリティ判定処理(S10A)を実行し、さらに、セキュリティデータを検証するためのテストパケットを送信する(S10B)。そのレスポンスに基づ

き、問い合わせ側代理システムXは、セキュリティデータが正しいか否かを判断する(S10C)。

【0156】そして、セキュリティデータが正しい場合、システムBは、入手した情報を信用できるものとし、その後の処理を続ける(S10D)。

【0157】以上述べたように、本実施形態では、問い合わせ側のシステムAに代えて、問い合わせ側代理システムVがセキュリティデータの問い合わせの代理を行う。また、返答側のシステムB等に代えて、返答側代理システムWがセキュリティデータを返答する。また、システムBは、問い合わせ側代理システムXおよび返答側代理システムYを通じて、入手した情報が信用できるか否かを判断する。

【0158】そのため、セキュリティデータの授受が問い合わせ側代理システムV(X)と返答側代理システムW(Y)との間に集約される。その結果、セキュリティデータを授受する際のトラフィックが低減される。また、返答側のシステムB(またはA)等は、個々の問い合わせに返答する手間を省略することができ、本来のアプリケーションの実行効率を向上できる。

【0159】<変形例>上記実施形態では、図16に示したように、問い合わせ側項目管理データベース5Aは、問い合わせ側代理システム22から参照された。しかし、これに代えて、例えば、問い合わせを行うシステムAが直接問い合わせ側項目管理データベース5Aを参照し、問い合わせを行うセキュリティデータの項目を決定してもよい。そして、システムAが問い合わせ側代理システム22に対してその項目の問い合わせを行うように依頼すればよい。

【0160】また、上記実施形態では、問い合わせ側代理システム22は、セキュリティデータの問い合わせを代理した。しかし、これに加えて、問い合わせ側代理システム22は、システムAからシステムB1、B2等への情報提供をも代行するようにしてもよい。

【0161】上記実施形態では、問い合わせ側のシステムAの代わりに問い合わせ側代理システム22を設け、返答側のシステムB1、B2等の代わりに返答側代理システム24を設けた。

【0162】しかし、本発明の実施は、このような構成には限定されない。例えば、返答側代理システム24を設けず、問い合わせ側代理システム22だけを設けてもよい。図16は、そのような情報システムのシステム構成図である。このシステムでは、上記実施形態と同様、問い合わせ側のシステムAから問い合わせ側代理システム22に問い合わせが依頼される。しかし、問い合わせ側代理システム22は、直接返答側システムB1、B2等に問い合わせを送信する。

【0163】また、例えば、問い合わせ側代理システム22等を設けず、返答側代理システム24だけを設けてもよい。図17にそのような構成の例を示す。この構成

では、問い合わせ側のシステムAは、返答側代理指定データベース23を参照し、返答側代理システム24に問い合わせを行う。

【0164】《コンピュータ読み取り可能な記録媒体》上記実施の形態におけるシステムA、B、問い合わせ側代理システムV、Xまたは返答側代理システムW、Yの機能をコンピュータに実現させるプログラムをコンピュータ読み取り可能な記録媒体に記録することができる。そして、コンピュータに、この記録媒体のプログラムを読み込ませて実行させることにより、上記実施の形態に示したシステムA、B、問い合わせ側代理システムV、Xまたは返答側代理システムW、Yとして機能させることができる。

【0165】ここで、コンピュータ読み取り可能な記録媒体とは、データやプログラム等の情報を電氣的、磁氣的、光学的、機械的、または化学的作用によって蓄積し、コンピュータから読み取ることができる記録媒体をいう。このような記録媒体のうちコンピュータから取り外し可能なものとしては、例えばフロッピー（登録商標）ディスク、光磁気ディスク、CD-ROM、CD-R/W、DVD、DAT、8mmテープ、メモリカード等がある。

【0166】また、コンピュータに固定された記録媒体としてハードディスクやROM（リードオンリーメモリ）等がある。

【0167】《搬送波に具現化されたデータ通信信号》また、上記プログラムをコンピュータのハードディスクやメモリに格納し、通信媒体を通じて他のコンピュータに配布することができる。この場合、プログラムは、搬送波によって具現化されたデータ通信信号として、通信媒体を伝送される。そして、その配布を受けたコンピュータを上記実施の形態に示したシステムA、B、問い合わせ側代理システムV、Xまたは返答側代理システムW、Yとして機能させることができる。

【0168】ここで通信媒体としては、有線通信媒体、例えば、同軸ケーブルおよびツイストペアケーブルを含む金属ケーブル類、光通信ケーブル等、または、無線通信媒体例えば、衛星通信、地上波無線通信等のいずれでもよい。

【0169】また、搬送波は、データ通信信号を変調するための電磁波または光である。ただし、搬送波は、直流信号でもよい。この場合、データ通信信号は、搬送波がないベースバンド波形になる。したがって、搬送波に具現化されたデータ通信信号は、変調されたブロードバンド信号と変調されていないベースバンド信号（電圧0の直流信号を搬送波とした場合に相当）のいずれでもよい。

【0170】《その他》更に、本実施の形態は以下の説明を開示する。

【0171】（付記1） ネットワークを利用し電子的に情報を送信または受信する通信装置であり、ネットワ

ークにアクセスする通信部と、通信を制御する制御部とを備え、前記制御部は、情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。（1）

（付記2） 前記システム情報には、相手装置の安全性に関連する情報が含まれており、前記制御部は、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かを判断する付記1記載の通信装置。（2）

（付記3） 前記制御部は、相手装置の安全性が所定の程度に確保されていないと判断したときに、その事実または理由を相手装置に通知する付記2記載の通信装置。

【0172】（付記4） 送受信される情報の種類と問い合わせるシステム情報の項目との関係を管理する情報項目管理部をさらに備え、前記制御部は、送受信する情報の種類に応じて、前記情報項目管理部からシステム情報の項目を選択し、相手装置に問い合わせる付記1または2記載の通信装置。

【0173】（付記5） 入手済みのシステム情報を管理する入手情報管理部をさらに備え、前記制御部は、前記入手情報管理部を参照し、その入手済みのシステム情報が相手装置において更新されているか否かを問い合わせ、更新されたシステム情報と未入手のシステム情報とを入手する付記1または2記載の通信装置。

【0174】（付記6） 前記入手情報管理部は、システム情報の項目ごとにそのシステム情報を入手した日時を管理し、前記制御部は、入手済みのシステム情報の項目にその入手日時を付加して相手装置に問い合わせる付記5記載の通信装置。

【0175】（付記7） 前記制御部は、相手装置から入手したシステム情報に基づき相手装置を検証する付記1記載の通信装置。（3）

（付記8） 前記制御部は、前記入手したシステム情報を検証するテストパケットを前記通信部から相手装置に対して送信し、そのテストパケットへのレスポンスが妥当か否かを判定することにより相手装置を検証する付記7記載の通信装置。（4）

（付記9） 送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行する通信装置であり、ネットワークにアクセスする通信部と、通信を制御する制御部とを備え、前記通信部は、送信元装置からの指令を受信し、前記制御部は、その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。

（5）

（付記10） 前記制御部は、前記相手装置に代えて、相手装置の処理を代行する代理装置に前記相手装置に係るシステム情報を問い合わせる付記9記載の通信装置。

【0176】(付記11) ネットワークを利用し電子的に情報を送信または受信する通信装置であり、ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、前記通信部は、送信元装置から当該通信装置に係るシステム情報の問い合わせを受信し、前記情報管理部は、問い合わせの対象となるシステム情報を管理し、前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記通信部から返答する通信装置。(6)

(付記12) 前記制御部は、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報を返答する付記11記載の通信装置。

【0177】(付記13) システム情報を更新した日時を管理する更新履歴管理部をさらに備え、前記通信部は、今回の問い合わせとその問い合わせに対する前回の返答日時とを受信し、前記制御部は、前回の返答日時と更新した日時とを比較し、前回の返答日時以降に更新されたシステム情報を返答する付記11記載の通信装置。

【0178】(付記14) 送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部と、システム情報を更新した日時を管理する更新履歴管理部とをさらに備え、前記制御部は、送信元装置から問い合わせがあったときに、その問い合わせに対する前回の返答日時とシステム情報を更新した日時と比較し、前回の返答日時の後に、更新されたシステム情報を返答する付記11記載の通信装置。

【0179】(付記15) 前記制御部は、問い合わせに対してシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しない付記11記載の通信装置。

【0180】(付記16) システム管理者の判断を促す入出力部をさらに備え、前記制御部は、問い合わせに対してシステム情報の返答可否を判断し、返答可否を決定できないシステム情報について、前記入出力部を通じて、システム管理者に返答可否の判断を促す付記11記載の通信装置。

【0181】(付記17) システム管理者の判断を促す入出力部をさらに備え、前記制御部は、問い合わせに対しシステム情報の返答可否を判断し、返答不可と判定されたシステム情報を返答をせず、返答可否を決定できないシステム情報についてシステム管理者に返答可否の判断を促す付記11記載の通信装置。

【0182】(付記18) 送信元装置の属性に係る情報を管理する送信元管理部をさらに備え、前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しない付記11記載の通信装置。(7)

(付記19) システム管理者の判断を促す入出力部を

さらに備え、前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、その送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促す付記18記載の通信装置。

【0183】(付記20) 送信元装置の属性に係る情報を管理する送信元管理部と、システム管理者の判断を促す入出力部とをさらに備え、前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報は返答をせず、返答可否を決定できないシステム情報についてはシステム管理者に返答可否の判断を促す付記11記載の通信装置。

【0184】(付記21) 送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行する通信装置であり、ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、前記通信部は、送信元装置から相手装置に係るシステム情報の問い合わせを受信し、前記情報管理部は、前記相手装置に係るシステム情報を管理し、前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記相手装置に代わって前記通信部から返答する通信装置。(8)

(付記22) 前記通信部は、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせを受信し、その代理装置に返答する付記21記載の通信装置。

【0185】(付記23) ネットワークを利用し電子的に情報を送信または受信する通信方法であり、情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有する通信方法。(9)

(付記24) 前記システム情報には、相手装置の安全性に関連する情報が含まれており、前記判断ステップでは、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かが判断される付記23記載の通信方法。

【0186】(付記25) 前記判断ステップにおいて、相手装置の安全性が所定の程度に確保されていないと判断されたときに、その事実または理由を相手装置に通知するステップをさらに有する付記24記載の通信方法。

【0187】(付記26) 送受信する情報の種類に応じて、問い合わせるシステム情報の項目を選択するステップをさらに有する付記23または24記載の通信方法。

【0188】(付記27) 入手済みのシステム情報を管理する入手情報管理部を参照する参照ステップと、その入手済みのシステム情報が相手装置において更新され

ているか否かを問い合わせる問い合わせステップと、更新されたシステム情報および未入手のシステム情報を入手するステップとをさらに有する付記23または24記載の通信方法。

【0189】(付記28) 前記入手情報管理部は、システム情報の項目ごとにその情報を入手した日時を管理しており、前記参照ステップでは、システム情報の項目ごとの入手日時が参照され、前記問い合わせステップでは、その入手日時が付加されてシステム情報の項目が問い合わせられる付記27記載の通信方法。

【0190】(付記29) 相手装置から返答されたシステム情報に基づき相手装置を検証する検証ステップをさらに有する付記23記載の通信方法。

【0191】(付記30) 前記入手したシステム情報を検証するテスト packets を前記相手装置に対して送信するステップをさらに有し、前記検証ステップでは、そのテスト packets へのレスポンスに基づき相手装置が検証される付記29記載の通信方法。

【0192】(付記31) 送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行する通信方法であり、前記送信元装置からの指令を受信するステップと、その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせる問い合わせステップと、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップとを有する通信方法。

【0193】(付記32) 前記問い合わせステップでは、前記相手装置に代えて、相手装置の処理を代行する代理装置に対して相手装置に係るシステム情報が問い合わせられる付記31記載の通信方法。

【0194】(付記33) ネットワークを利用し電子的に情報を送信または受信する通信方法であり、送信元装置からシステム情報の問い合わせを受信する受信ステップと、問い合わせに対するシステム情報を検索するステップと、そのシステム情報を返答する返答ステップとを有する通信方法。

【0195】(付記34) 前記返答ステップでは、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報が返答される付記33記載の通信方法。

【0196】(付記35) システム情報を更新した日時を管理する更新履歴管理部を参照するステップと、前回の問い合わせに対する返答日時とシステム情報を更新した日時とを比較するステップとを有し、前記受信ステップでは、問い合わせとともに前回の問い合わせに対する返答日時を受信し、前記返答ステップでは、その返答日時以降に更新されたシステム情報が返答される付記33記載の通信方法。

【0197】(付記36) 送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合

わせに対する返答日時を管理する返答履歴管理部を参照するステップと、送信元装置から問い合わせがあったときに、前回の返答日時とシステム情報を更新した日時とを比較するステップとをさらに有し、前記返答ステップでは、前回の返答日時の後に、更新されたシステム情報が返答される付記33記載の通信方法。

【0198】(付記37) 問い合わせに対しシステム情報の返答可否を判断するステップをさらに有し、返答不可と判断されたシステム情報が返答されない付記33記載の通信方法。

【0199】(付記38) 返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記37記載の通信方法。

【0200】(付記39) 送信元装置の属性に係る情報を管理する送信元管理部を検索するステップと、前記送信元装置に応じて返答可否を判断するステップとを有する付記33記載の通信方法。

【0201】(付記40) 前記送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記39記載の通信方法。

【0202】(付記41) 送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行する通信方法であり、前記送信元装置からの相手装置に係るシステム情報の問い合わせを受信する受信ステップと、問い合わせに応じて、前記相手装置に係るシステム情報を検索するステップと、前記相手装置に代わって通信部から返答するステップとを有する通信方法。

【0203】(付記42) 前記受信ステップでは、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせを受信される付記41記載の通信方法。

【0204】(付記43) コンピュータに、ネットワークを利用し電子的に情報を送信または受信させるプログラムであり、情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。(10)

(付記44) 前記システム情報には、相手装置の安全性に関連する情報が含まれており、前記判断ステップでは、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かが判断される付記43記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0205】(付記45) 前記判断ステップにおいて、相手装置の安全性が所定の程度に確保されていないと判断されたときに、その事実または理由を相手装置に

通知するステップをさらに有する付記44記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0206】(付記46) 送受信する情報の種類に応じて、問い合わせるシステム情報の項目を選択するステップをさらに有する付記43または44記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0207】(付記47) 入手済みのシステム情報を管理する入手情報管理部を参照する参照ステップと、その入手済みのシステム情報が相手装置において更新されているか否かを問い合わせる問い合わせステップと、更新されたシステム情報および未入手のシステム情報を入手するステップとをさらに有する付記43または44記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0208】(付記48) 前記入手情報管理部は、システム情報の項目ごとにその情報を入手した日時を管理しており、前記参照ステップでは、システム情報の項目ごとの入手日時が参照され、前記問い合わせステップでは、その入手日時が付加されてシステム情報の項目が問い合わせられる付記47記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0209】(付記49) 相手装置から返答されたシステム情報に基づき相手装置を検証する検証ステップをさらに有する付記43記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0210】(付記50) 前記入手したシステム情報を検証するテストパケットを前記相手装置に対して送信するステップをさらに有し、前記検証ステップでは、そのテストパケットへのレスポンスに基づき相手装置が検証される付記49記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0211】(付記51) コンピュータに、送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行させるプログラムであり、前記送信元装置からの指令を受信するステップと、その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせる問い合わせステップと、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0212】(付記52) 前記問い合わせステップでは、前記相手装置に代えて、相手装置の処理を代行する代理装置に対して相手装置に係るシステム情報が問い合わせられる付記51記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0213】(付記53) コンピュータに、ネットワークを利用し電子的に情報を送信または受信させるプログラムであり、送信元装置からシステム情報の問い合わせを受信する受信ステップと、問い合わせに対するシステム情報を検索するステップと、そのシステム情報を返

答する返答ステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0214】(付記54) 前記返答ステップでは、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報が返答される付記53記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0215】(付記55) システム情報を更新した日時を管理する更新履歴管理部を参照するステップと、前回の問い合わせに対する返答日時とシステム情報を更新した日時とを比較するステップとを有し、前記受信ステップでは、問い合わせとともに前回の問い合わせに対する返答日時を受信し、前記返答ステップでは、その返答日時以降に更新されたシステム情報が返答される付記53記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0216】(付記56) 送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部を参照するステップと、送信元装置から問い合わせがあったときに、前回の返答日時とシステム情報を更新した日時とを比較するステップとをさらに有し、前記返答ステップでは、前回の返答日時の後に、更新されたシステム情報が返答される付記53記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0217】(付記57) 問い合わせに対しシステム情報の返答可否を判断するステップをさらに有し、返答不可と判断されたシステム情報が返答されない付記53記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0218】(付記58) 返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記57記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0219】(付記59) 送信元装置の属性に係る情報を管理する送信元管理部を検索するステップと、前記送信元装置に応じて返答可否を判断するステップとを有する付記53記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0220】(付記60) 前記送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記59記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0221】(付記61) コンピュータに、送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行させるプログラムであり、前記送信元装置からの相手装置に係るシステム情報の問い合わせを受信する受信ステップと、問い合わせに応じて、前記相手装置に係るシステム情報を検索するステップと、前記相手装

置に代わって通信部から返答するステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0222】（付記62） 前記受信ステップでは、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせが受信される付記61記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0223】

【発明の効果】以上説明したように、本発明によれば、通信相手の安全性を確認した上で通信することができる。

【図面の簡単な説明】

【図1】 本発明の第1実施形態におけるセキュリティレベルの確認を行う情報システムの構成図

【図2】 問い合わせ項目管理データベースのデータ構造を示す図

【図3】 入手データ管理データベースのデータ構造を示す図

【図4】 返答可否データベースのデータ構造を示す図

【図5】 セキュリティデータ管理データベースのデータ構造を示す図

【図6】 問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート

【図7】 セキュリティデータの問い合わせ処理の詳細を示すフローチャート

【図8】 セキュリティデータの返答処理の詳細を示すフローチャート

【図9】 セキュリティ判定処理の詳細を示すフローチャート

【図10】 第1実施形態の変形例における返答履歴管理

データベースのデータ構造を示す図

【図11】 第1実施形態の変形例における情報を過去に提供した日時と変更した日時を確認する処理示す図

【図12】 第2実施形態に係る情報システムのシステム構成図

【図13】 返答側代理指定データベース23のデータ構成を示す図

【図14】 第2実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート（1）

【図15】 第2実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート（2）

【図16】 第2実施形態の変形例に係る情報システムのシステム構成図（1）

【図17】 第2実施形態の変形例に係る情報システムのシステム構成図（2）

【符号の説明】

A、B システム

2 中央制御部

3 情報処理部

4 セキュリティデータチェック部

5 データベース

6 入出力部

7 ネットワークインターフェース

12、13 管理者端末

21 問い合わせ側代理指定ファイル

22、V、X 問い合わせ側代理システム

23 返答側代理指定データベース

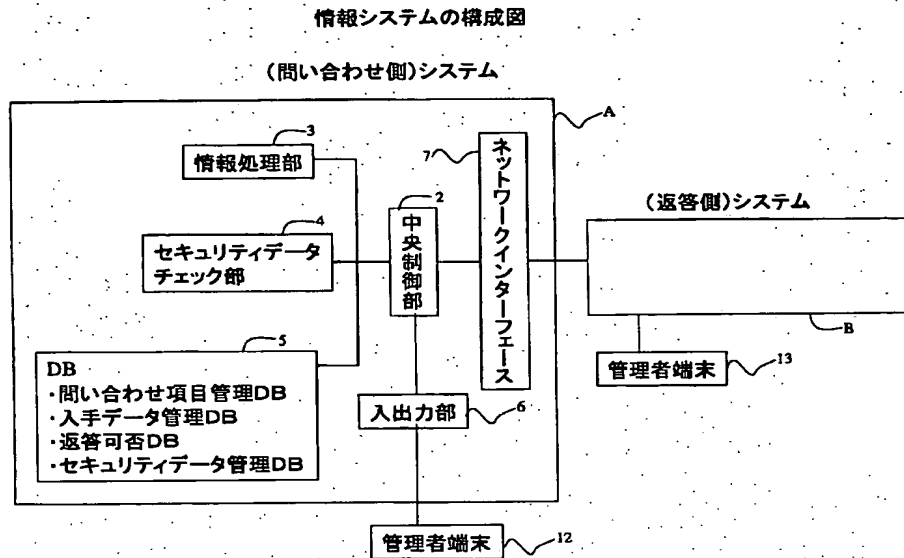
24、W、Y 返答側代理システム

【図2】

問い合わせ項目管理データベース

授受される情報の種類	必要なセキュリティデータ項目
1000万円未満の取引 1000万円以上の取引 関係者外秘情報 情報A	OS、パスワード暗号化 OS、パスワード暗号化、ログ監査、項目A OS、開いているポート、ウイルス対策、ログ監査 開いているポート、パスワード暗号化、項目A

【図1】



【図3】

入手データ管理データベース

返答側システム	項目	入手日時	入手セキュリティデータ
システムB	OS	2000.9.14 09:00	Windows NT SP5
システムB	開いているポート	1999.11.9 17:32	7, 23, 80
システムB	ログ監査頻度	2000.9.17 01:04	1回/1日
システムB	項目A	2000.4.4	データA
システムC	OS	1999.1.25 03:57	Linux 2.2.8
システムC	パスワード暗号化	2000.10.5 14:24	している

【図5】

セキュリティデータ管理データベース

項目	セキュリティデータ	更新日時
OS	Windows NT SP5	2000.1.13 11:00
開いているポート	7, 23, 80	2000.3.31 12:24
ウィルス対策	Norton Anti Virus	2000.2.24 15:28
ログ監査頻度	1回/1日	1996.12.6 07:32
パスワード暗号化	している	1998.9.14 14:12
項目A	データA	1999.12.4 09:07

【図13】

返答側代理指定データベース

返答側システム	返答側代理システム
B1	D1
B2	D1
B3	D2

【図4】

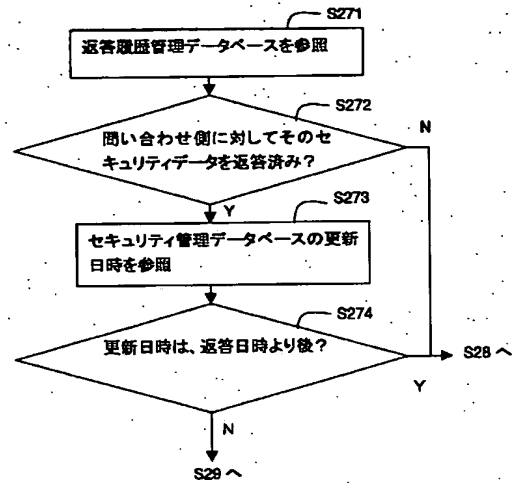
返答可否データベース

問い合わせ側システム	項目	判断
システムA	OS	×
システムA	開いているポート	○
システムA	ウィルス対策	○
システムA	ログ監査頻度	○
システムA	パスワード暗号化	○
システムA	項目A	×
システムC	OS	△
システムC	開いているポート	○
システムC	ウィルス対策	×
システムC	ログ監査頻度	○
システムC	パスワード暗号化	○
システムA	項目A	×

○: 返答してよい
 ×: 返答してはいけない
 △: 返答可否の判断不可

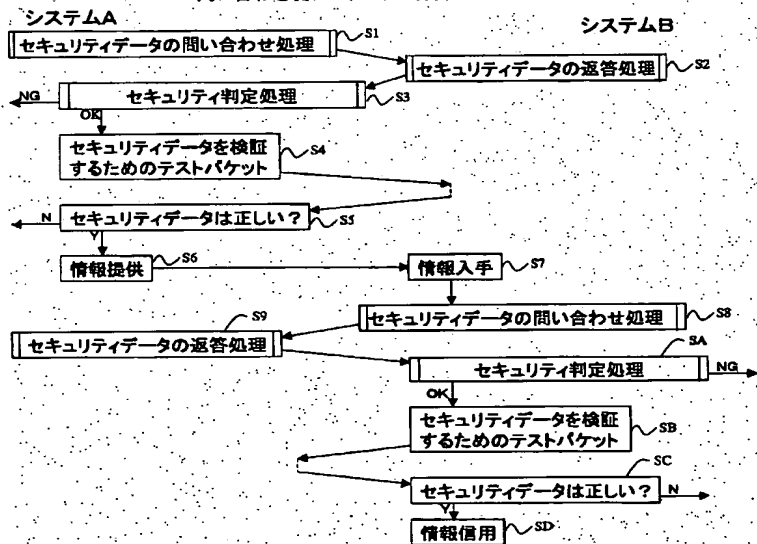
【図11】

過去に提供をした日時と変更した日時を確認する処理(変形例)



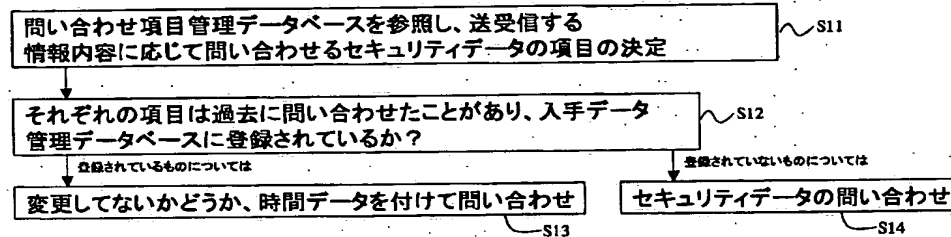
【図6】

問い合わせ側システムと返答側システムとの通信手順



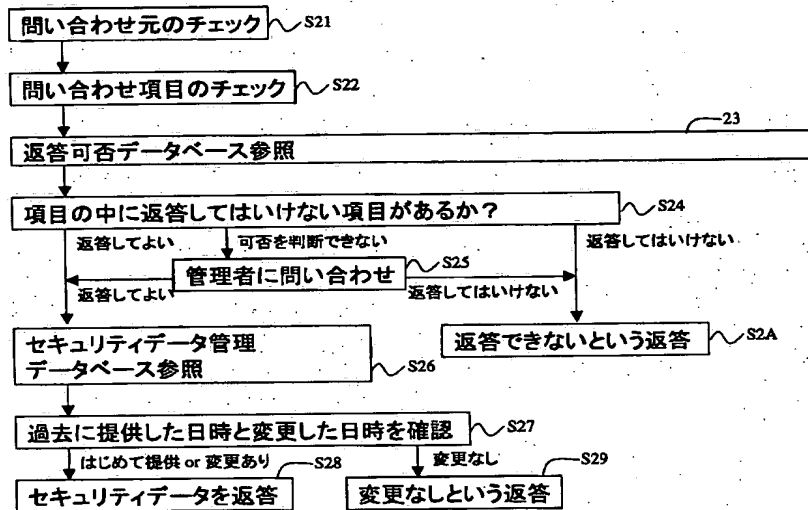
【図7】

セキュリティデータの問い合わせ処理



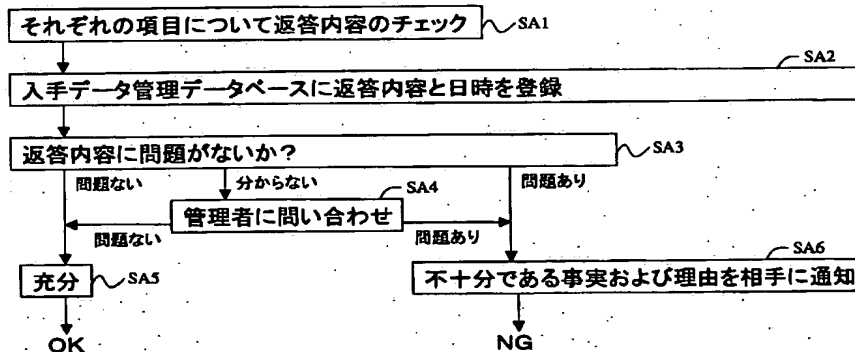
【図8】

セキュリティデータの返答処理



【図9】

セキュリティ判定処理



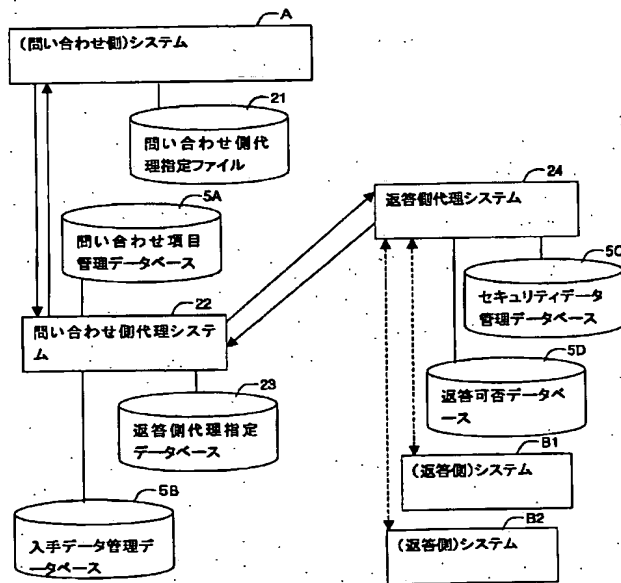
【図10】

返答履歴管理データベース

問い合わせ側システム	項目	返答日時	返答セキュリティデータ
システムA	OS	2000.9.14 09:00	Windows NT SP5
システムA	開いているポート	1999.11.9 17:32	7, 23, 80
システムA	ログ監視頻度	2000.9.17 01:04	1回/1日
システムA	項目A	2000.4.4	データA
システムC	OS	1999.1.25 03:57	Linux 2.2.8
システムC	パスワード暗号化	2000.10.5 14:24	している

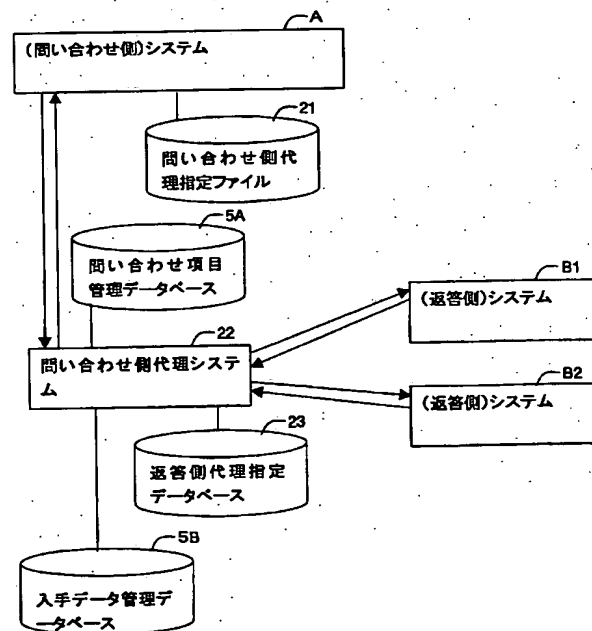
【図12】

第2実施形態に係る情報システムのシステム構成図



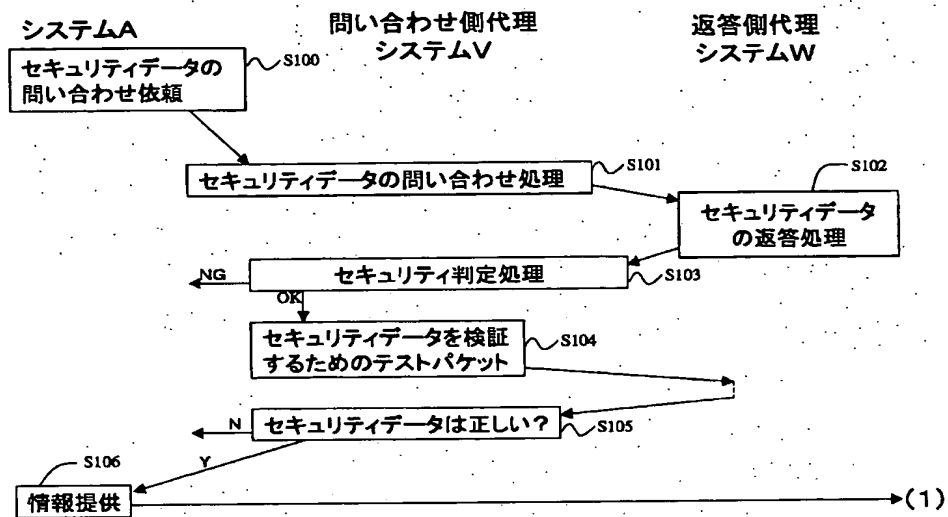
【図16】

第2実施形態の変形例に係る情報システムのシステム構成図



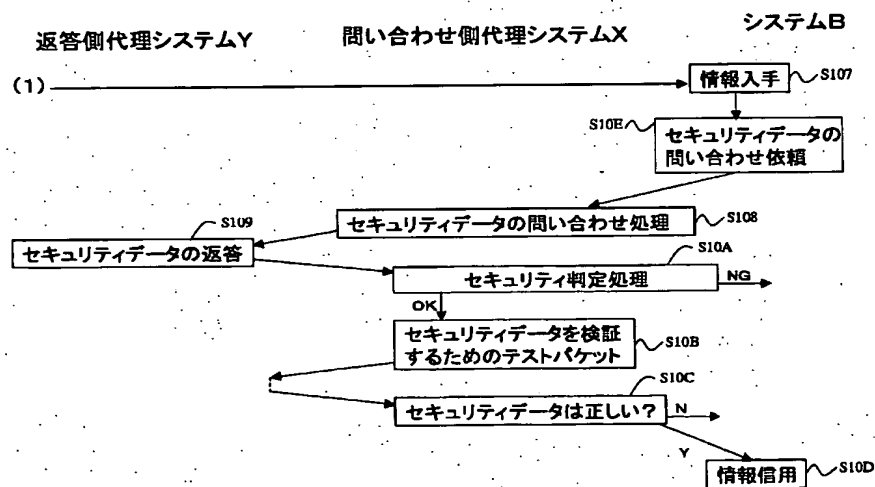
【図14】

第2実施形態における問い合わせ側システムと返答側システムとの通信手順1

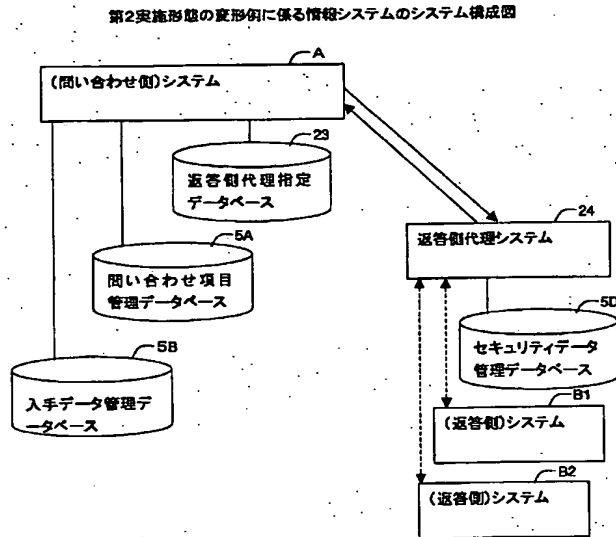


【図15】

第2実施形態における問い合わせ側システムと返答側システムとの通信手順2



【図17】



フロントページの続き

(72)発明者 黒田 康嗣
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内
 (72)発明者 小谷 誠剛
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内

Fターム(参考) 5K030 GA15 HA08 JT03 KA01 KA13
 LD19
 5K034 AA05 BB06 DD01 FF01 HH01
 HH02 HH13 LL01 TT02
 5K035 AA03 BB01 CC06 DD02 EE00
 FF02 GG01 JJ04 MM03